Questions For Board Members to Ask About Information Security

From Pat Carbine's presentation at the White House on April 18, 2000
(PricewaterhouseCoopers assisted in providing these questions.)

- Does the company have a chief information technology officer? Why not?
- Does the company have a chief information technology security officer? Why not?
- Does the company consider itself an industry leader in the use of information technology?
- What are the budgeted capital expenditures for information technology this year? Next year? How does this compare with other companies in the industry?
- How is the company keeping up with changes in information technology?
- Are the company's management information systems state of the art, or will significant investments be needed to maintain the company's competitiveness?
- Does the company measure the relative investment in its information technology systems to benchmark expenditures as well as performance against those of its peers?
- Does the company outsource key technology functions? Is it considering this?
- When was the last time the company's information technology controls were reviewed? Was the evaluation performed by an outside consultant? What were the results? Have all recommendations been implemented? If there has been no recent review, is one scheduled?
- Does the company have a business continuity plan in the event its information technology systems are disabled? Has the plan been tested? When? What were the results?
- Are controls and security surrounding the company's computer operations sufficient to prevent unauthorized access to computer files, alterations of records, loss or theft of computer data and trade secrets and misappropriation of assets?
- Has the company been a victim of computer fraud by employees or others?
- Is the company vulnerable to computer viruses? What steps have been taken to determine if the company detects attacks and responds in a timely manner?
- Did the external auditors and/or the internal auditors review computer systems and controls? What were the results of their reviews?
- Have hackers succeeded in breaking into the company's computer systems? How did it happen? Have we gone through the drill of retaining professional hackers to test our systems?
- With the continued migration from mainframe legacy systems to client server systems using packaged software, does the company have adequate controls over program documentation and changes, security, operations, and monitoring?
- Has the company, if we're doing business globally, upgraded its information systems for the introduction of the Euro?

On the subject of E-Business:

- What are the company's e-business plans?
- What are the major threats and opportunities to the company from e-business?
- Has the business lost market share to new companies or traditional competitors that are using e-business more effectively? Does the company have adequate risk management policy and controls over its e-business?
- What steps have been taken to ensure privacy of customer information on the web site(s)?
- Does the company web site prominently disclose its e-business practices for its customers?
- Do we have an individual assigned responsibility for establishing strategy, security direction, and associated policy and awareness?
- Is there an overall enterprise security policy? Or is it dispersed to different organizational units?
- How are systems under development evaluated for proper security features? Is there a standard process for this within the development process?
- What security or privacy mechanisms are in place with business partners, agents and suppliers? Do those entities directly utilize our systems and/or data? How are they introduced to our policies?